III. REMARKS

1. Claims 19, 21, 23-26, 28, 31-48, 55-59, 61-64, 66-70, 74-82, 84-94, 96, and 133-135 are still pending in the application. Claims 122, 124 - 126, 128, 130, 132, and 136-156 have been cancelled. Claims 19, 21, 23-26, 28, 31-35, 44-48, 55-59, 61-64, 68-70, 82, 84-85, 94, 96 and 133 have been amended.

2. Summary of Official Action

2.1 In point 8 of the current Official Action, issued by the USPTO on 4 December 2009, claim 156 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. (US Patent 5,502,767) in view of Talbot (U.S. Patent 4,555,805)

2.2 In point 9, claims 19, 21, 23, 28, 31, 36, 44, 46-48, 55-59, 61-62, 66, 68, 74, 77-79, 81-82, 84-87, 90-91, 93-94, 96, 122, 124, 128, 132-134, 136-139, 142-143, 148 and 152-153 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al. (U.S. Patent 5,502,767) and further in view of Talbot (U.S. Patent 4,555,805) and Rasmussen et al (U.S. Patent 5,222,136).

2.3 In point 10, claims 24-26, 63-64 and 135 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot and Rasmussen et al. and further in view of Billstrom et al. (U.S. Patent 5,590,133).

2.4 In point 11, claims 32-34, 67, 69, 97, and 144-146 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot and Rasmussen et al. and further in view of Lewis et al. (U.S. Patent 6,192,255).

2.5 In point 12, claims 35 and 70 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot and Rasmussen et al. and further in view of Kniffin et al. (U.S. Patent 6,072,402).

2.6 In point 13, claim 45 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot and Rasmussen et al. and further in view of Serbetciouglu et al. (U.S. Patent 5,719,918).

2.7 In point 14, claims 37-43, 75-76, 80, 87-89, 92, 125-126, 130, 149-151, and 154-155 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot and Rasmussen and further in view of Kennedy et al., European Patent 0 680 171.

2.8 In point 15, claims 140-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot and Rasmussen in view of Raith (U.S. Patent 5,237,612).

2.9 And, in point 16, claim 147 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sasuta et al., Talbot and Rasmussen in view of Fujiwara et al. (U.S. Patent 5,266,947).

3. Applicant's Response to the Official Action

In the following, the Applicant presents arguments in favour of the patentability of the amended independent claims, that is, claims 19, 59, 82, 85 and 94. As dependent claims include all the features of the claim(s) from which they depend, it is the Applicant's view that demonstrating the patentability of the independent claims is sufficient to demonstrate the patentability of the dependent claims as well.

3.1 Applicants note that claim 156 has been cancelled rendering the rejection moot.

3.2 Applicants respectfully submit that claims 19, 21, 23, 28, 31, 36, 44, 46-48, 55-59, 61, 62, 66, 68, 74, 77-79, 81, 82, 84-87, 90, 91, 93, 94, 96, 133, and 134 are patentable over the combination of Sasuta, Talbot and Rasmussen et al. (US 5,222,136, "Rasmussen") under 35 USC 103(a).

Independent claims 19, 59, 82, 85 and 94 are included in this rejection. The Applicant's arguments will therefore focus on distinguishing newly amended independent claims 19, 59, 82, 85 and 94, from the art cited in this rejection.

In Point 9 of the present Final Office Action, with reference specifically to independent claims 19, 59 and 82, the Examiner asserts that column 3, lines 23-29, column 3, line 60 to column 4, line 17 and Figure 1 of the Sasuta patent disclose (in the words of the previously submitted claims) *"monitoring at the mobile station control signals received from the mobile communication network to detect a cipher mode command message, the cipher mode command message requesting the mobile station to start enciphering"*.

Referring to independent method claim 19 of the newly-submitted claims, this limitation has now been amended to read: *"monitoring ~~at~~by ~~the~~a mobile station in the mobile communication network of network control signals received by the mobile station from the mobile communication network over an air interface to detect a cipher mode command message, the cipher mode command message configured to requesting the mobile station to start enciphering of user data"* (where the newly-made amendments are shown with change-tracking).

It should be appreciated that the newly-made amendments to this claim feature are intended purely for the purposes of clarifying the claimed subject matter.

It is the Applicant's view that the cited passages of Sasuta (column 3, lines 23-29, column 3, line 60 to column 4, line 17 and Figure 1) do not disclose this feature of claim 19 (or the equivalent features of the other independent claims). More specifically, it should be noted that the "encryption indication" referred to in the aforementioned passages and shown in Figure 1, relates to an information field provided **on the control channel** of Sasuta's system to indicate whether information **on the control channel** is being transmitted in secure or non-secure mode (see Sasuta, column 4, lines 4-11). It is clear from the paragraphs referred to by the Examiner that the purpose of this indication is purely to indicate whether particular information transmitted on the control channel is encrypted or not. Thus, Sasuta's "encryption indication" does not perform the role of requesting a mobile station to "....start enciphering of user data" (data that would be transmitted on a working channel in Sasuta), as required by the newly amended independent claims.

Furthermore, as can be seen readily from Figure 1 of Sasuta, no corresponding or equivalent indication is provided on the working channel of Sasuta and, in general, the whole of Sasuta's disclosure assumes that communication on the working channel is performed in a secure or encrypted manner. In fact, Sasuta is completely silent concerning the manner in which enciphered communication **on the working channel is started.**

Neither can Sasuta's encryption indication **on the control channel** be interpreted as *"an indication that said enciphered mode of communication for user data is set on in the mobile communication network"*, as required by the newly-amended independent claims since, according to Sasuta, the encryption indication is relevant only for information transmitted on the control channel. For these reasons, it is the Applicant's view that Sasuta cannot provide the

skilled person with any teaching relevant to **starting enciphering of user data**, as required by the newly-amended independent claims.

Turning now to Talbot, the Examiner asserts that column 11, line 59 to column 12, line 3; column 8, lines 3 to 25 and column 9, lines 39-50 of the Talbot patent disclose (in the words of the previously submitted claims) *"....indicating to a user of the mobile station that the mobile communication network is operating in an enciphered mode of communication...."*. The Applicant respectfully disagrees with this point of view.

In the newly-amended claims, this element of independent claim 19 has been amended to read: *"indicating to a user of the mobile station that ~~the mobile communication network is operating in an~~said enciphered mode of communication for user data is set on in the mobile communication network, using a cipher mode indicator provided in the mobile station"* (where the newly-made amendments shown with change-tracking). Equivalent amendments have been made to the other independent claims.

It is the Applicant's view that the cited passages of text from Talbot do not disclose this element of the independent claims. More specifically, the referenced passages of Talbot refer to tone signaling conducted between the calling and called parties during call establishment (column 11, line 59 to column 12, line), switching between signaling and output lines in a mobile station when a secure connection is established (column 8, lines 3 to 25) and determining that a called party has answered a call by detecting lifting of a handset (column 9, lines 39 to 50). The latter part of this passage (specifically, column 9, lines 43 to 48) refers to an alternative arrangement in which a terminal (21) in the telecommunications network may wait for a secure service request from a calling or called party, thereby allowing users to decide if they wish to accept higher billing expenses that may be associated with a secure mode of communication.

Addressing these points in turn, it should be appreciated that in Talbot the tone signaling used during call establishment is not routed through the secure voice module (SVM). This can be seen from both the base station and mobile station block diagrams presented in Figure 1 and is stated explicitly in the text between column 5, line 63 and column 6, line 2. As a result, the tone signaling to and from the base station passes directly to and from the terminal (21) in a conventional manner (column 5, lines 65 to 67). It is therefore the Applicant's view that the tone signaling that takes place during call setup **would not be audible** to the called or calling party.

Such signaling cannot therefore be invoked as a disclosure of providing an **indication** to a user as required by the claims, since the user would not be able hear it.

Furthermore, even if the tone signaling were audible to the calling or called party, the most the calling party would hear might possibly be a conventional "dialing tone" when picking up a handset to dial a number and a "ringing tone" when the call is connected to the correct called line. As is known from conventional telephone systems, neither of these signals provides any indication of whether an "....*enciphered mode of communication for user data is set on in the mobile communication network".*

Considering the recording of information that a secure connection exists so that the parties to the call can be billed for the added service (column 11, line 67 to column 12, line 2 of Talbot), the Applicant would point out that there is no teaching or suggestion in Talbot that any indication of the additional cost would be provided to either one of the parties either immediately before or during a secure call.

Of course, according to Talbot, a called or calling or called party requesting a secure call would be aware of his / her decision to request a secure call, but Talbot provides no teaching or suggestion that this decision to select a secure mode of communication would be indicated to either of the parties to the call *"....using a cipher mode indicator provided in the mobile station"*, as required by the independent claims.

Furthermore, Talbot does not suggest that billing information is provided in real time. Considering the priority date of Talbot (March 1980), the Applicant would suggest that most likely the billing information referred to by Talbot would be provided in an entirely conventional manner, e.g. a written paper statement delivered by post at some considerable time after the secure communication being billed. Such a bill cannot be considered in any way to fulfill the claimed requirement of *"indicating to a user of the mobile station that said enciphered mode of communication for user data is set on in the mobile communication network, using a cipher mode indicator provided in the mobile station"*. Any assumption on the part of the Examiner that Talbot discloses e.g. the display of billing information in real time at the mobile terminal is not supported in any way by Talbot's disclosure and would represent an impermissible use of hindsight.

It is also the Applicant's view that Talbot lacks any disclosure of a *"cipher mode command message, the cipher mode command message configured to requesting the mobile station to start enciphering of user data"*, since, according to Talbot a receiving mobile station simply switches over to an enciphered mode of communication whenever enciphered voice data is received and deciphered data is present at the output of the secure voice module (column 8, lines 5 to 23). Thus Talbot cannot compensate for the lack of this claimed feature in Sasuta.

Finally, turning to Rasmussen, the Examiner asserts that this newly-introduced document discloses the limitation of *"indicating to a user of the mobile station that the mobile communication network is operating in an enciphered mode of communication, using a cipher mode indicator provided in the mobile station"*. In newly-amended independent method claim 19, for clarification, this feature of the claim has been amended to read: *"indicating to a user of the mobile station that the mobile communication network is operating in ansaid enciphered mode of communication for user data is set on in the mobile communication network, using a cipher mode indicator provided in the mobile station* (where, once more, the newly-made amendments are shown with change-tracking). Corresponding amendments have been made to the other independent claims.

In the Applicant's view, Rasmussen specifically teaches away from the presently claimed solution and, for this reason, would not be considered by the skilled person.

More specifically, in the background section of his patent, Rasmussen teaches that providing separate security systems to protect each type of communication device (e.g. telephones, fax machines, and computers) in an office environment is unduly expensive (column 1, lines 65 to 67). As a solution to this problem, Rasmussen suggests coupling the various devices which may require secure communications to a single encrypted communication device (ECOM) which is responsible for conducting encrypted communications across an otherwise unciphered communication network with a corresponding ECOM at a remote location (see Figure 1 of Rasmussen and associated description). This clearly teaches away from integrating encryption and display functionalities in any one of the various devices, and would therefore also teach away from providing in a mobile station the claimed features relating to monitoring network control signals, interpreting the monitored network control signals, starting enciphering and indicating that an enciphered mode of communication for user data is set on in a mobile communication network. Furthermore, it is the Application's view that Rasmussen's ECOM itself

cannot be considered a mobile station in the sense of the presently claimed invention. More particularly, an ECOM according to Rasmussen is not free to move without restriction e.g. within the bounds of a mobile communication network, because its physical location is dictated by the location of the devices for which it provides encrypted communications, so it cannot be considered itself as "a mobile station".

Additionally, it is also the Applicant's view that Rasmussen's system is not capable of providing a solution to the problem identified in the present application and also for this reason would not be considered by the skilled person. In particular, it should be noted that Rasmussen's ECOM units provide a mechanism for conducting secure communications over a network that is essentially "open" or unsecured. Secure communications can therefore only take place between corresponding ECOM units at respective transmitting and receiving sites. Although the ECOMs at either end of the communication path through the network have displays, the visual indication provided on those displays relates to a status of communication between the ECOMs and does not provide the user with an indication that an *"enciphered mode of communication for user data is set on in the mobile communication network".* Indeed it cannot do so since in Rasmussen the network itself is not configured to provide network control signals that request the use of an enciphered mode of communication. Thus, because Rasmussen's ECOM is essentially not a mobile station and the users of Rasmussen communication network know that the network itself can only provide unsecured communication, the skilled person would not be motivated to consult Rasmussen's teachings when seeking to solve the problem of how to make users of mobile stations aware of whether or not an enciphered mode of communication is set on or off in a mobile communication network, as they connect to and move within the network.

Given the lack of disclosure of claimed features in the teachings of Sasuta (no cipher mode command message, no indication to a user) and Talbot (no cipher mode command message, no indication to a user), and the fact that Rasmussen actually teaches away from the solution provided by the presently claimed invention and is incompatible with the problem to be solved, it is the Applicant's view that the skilled person would not seek to make the combination suggested by the Examiner. In fact, this would seem to be a mere mosaic-like juxtaposition of features without clear motivation to make the suggested association of teachings. Furthermore, if despite the clear teachings to the contrary and the incompatibility of Rasmussen, the skilled person would nevertheless attempt to make the suggested combination, the resulting system

would not fall within the scope of the currently amended claims, at least due to the aforementioned lacking features in Talbot and Sasuta.

At least for the aforementioned reasons, the Applicant believes the current independent claims to be patentably distinct from the proposed combination of Sasuta, Talbot, and Rasmussen and respectfully requests reconsideration of the application.

Therefore, the combination of Sasuta, Talbot and Rasmussen fails to render claims claims 19, 21, 23, 28, 31, 36, 44, 46-48, 55-59, 61, 62, 66, 68, 74, 77-79, 81, 82, 84-87, 90, 91, 93, 94, 96, 133, and 134 unpatentable.

3.3 Applicants respectfully submit that claims 24-26, 63, 64, and 135 are patentable over the combination of Sasuta, Talbot, Rasmussen and Billstrom et al. (US 5,590,133, "Billstrom") under 35 USC 103(a).

Billstrom fails to disclose or suggest the features of the independent claims missing from the combination of Sasuta, Talbot, and Rasmussen. Therefore, the combination of Sasuta, Talbot, Rasmussen and Billstrom fails to render claims 24-26, 63, 64, and 135 unpatentable.

3.4 Applicants respectfully submit that claims 32-34, 67, and 69 are patentable over the combination of Sasuta, Talbot, Rasmussen and Lewis et al. (US 6,192,255, "Lewis") under 35 USC 103(a).

Lewis fails to disclose or suggest the features of the independent claims missing from the combination of Sasuta, Talbot, and Rasmussen. Therefore, the combination of Sasuta, Talbot, Rasmussen, and Lewis and fails to claims 32-34, 67, and 69 unpatentable.

3.5 Applicants respectfully submit that claims 35 and 70 are patentable over the combination of Sasuta, Talbot, Rasmussen and Kniffin et al. (US 6,072,402, "Kniffin") under 35 USC 103(a).

Kniffin fails to disclose or suggest the features of the independent claims missing from the combination of Sasuta, Talbot, and Rasmussen. Therefore, the combination of Sasuta, Talbot, Rasmussen, and Kniffin fails to render claims 35 and 70 unpatentable.

3.6 Applicants respectfully submit that claim 45 is patentable over the combination of Sasuta, Talbot, Rasmussen and Serbetciouglu et al. (US 5,719,918, "Serbetciouglu") under 35 USC 103(a).

Serbetciouglu fails to disclose or suggest the features of the independent claims missing from the combination of Sasuta, Talbot, and Rasmussen. Therefore, the combination of Sasuta, Talbot, Rasmussen, and Serbetciouglu fails to render claim 45 unpatentable.

3.7 Applicants respectfully submit that claims 37-43, 75, 76, 80, 87-89, and 92 are patentable over the combination of Sasuta, Talbot, Rasmussen and Kennedy et al. (EP 0680171A2, "Kennedy") under 35 USC 103(a).

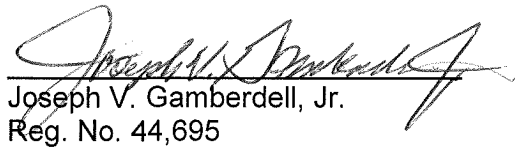
Kennedy fails to disclose or suggest the features of the independent claims missing from the combination of Sasuta, Talbot, and Rasmussen. Therefore, the combination of Sasuta, Talbot, Rasmussen, and Kennedy fails to render claims 37-43, 75, 76, 80, 87-89, and 92 unpatentable.

3.8 Applicants note that claims 140, 141, 147 156 has been cancelled rendering the rejection of these claims moot.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,



4 June 2010

Joseph V. Gamberdell, Jr.
Reg. No. 44,695

Perman & Green, LLP
99 Hawley Lane
Stratford, CT 06614
(203) 259-1800
Customer No.: 2512

Date